PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-105058
(43)Date of publication of application : 24.04.1998

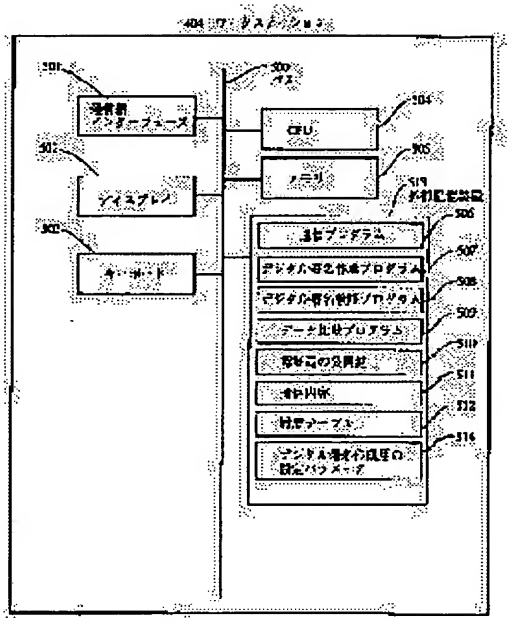
(51)Int.Cl. G09C 1/00

(21)Application number : 08-254057
(22)Date of filing : 26.09.1996

(71)Applicant : HITACHI SOFTWARE ENG CO LTD
(72)Inventor : TSUTSUMI TOSHIYUKI

(54) DATA GUARANTEE SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To secure the perfectness of data guaranteed by a transmitter even when these data are inspected by calculating a digital signature for newly guaranteeing the perfectness of communication contents by returning the communication contents deleted/changed by an inspector or an inspection process to the transmitter.
SOLUTION: The transmitter stores the copy of two pieces of received data in the history table of an external storage device 513. Next, the transmitter executes a digital signature preparation program 507 in an external storage device 513 of a work station 404 on a memory 505 of the work station 404 by applying the setting parameter for digital signature preparation of the work station 404 to be uniquely determined by a unidirectional function algorithm identifier contained in the received communication data to this program 507 and calculates the digital signature of the transmitter corresponding to the confirmed inspected communication contents. Afterwards, the transmitter prepares communication data in prescribed data structure from the confirmed inspected communication data and the selected digital signature and transmits these data.



LEGAL STATUS

[Date of request for examination]	12.06.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3476171
[Date of registration]	26.09.2003
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－105058

(43)公開日　平成10年(1998)４月24日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｚ
			６４０Ｄ
			６４０Ｅ

審査請求　未請求　請求項の数１　ＯＬ　（全 13 頁）

(21)出願番号　特願平8－254057

(22)出願日　平成８年(1996)９月26日

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地

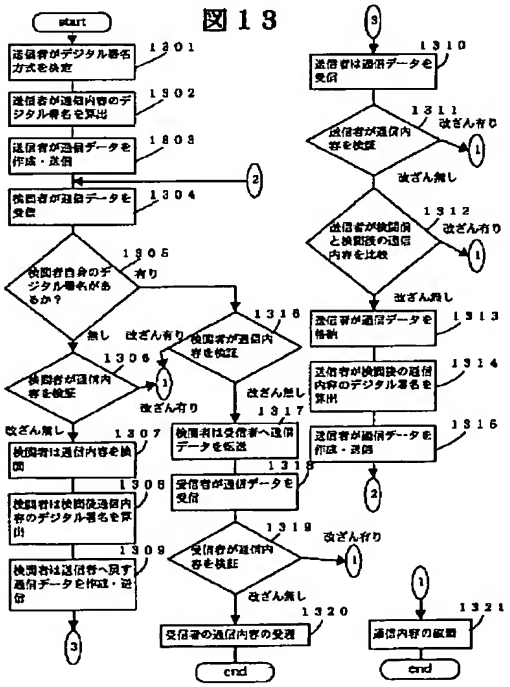
(72)発明者　堤　俊之
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(74)代理人　弁理士　秋田　収喜

(54)【発明の名称】　データ保証システム

(57)【要約】
【課題】　送信者と受信者の間で通信される通信内容が途中通信経路の端末で検閲され、削除されるシステムであって、検閲された通信内容であっても、受信者が送信者の保証したデータのデータの完全性を確認できる。
【解決手段】　検閲者もしくは、検閲プロセスが修正・変更した通信内容を送信者に戻して新たに通信内容の一貫性を保証するデジタル署名を計算する。

図１３



1

【特許請求の範囲】

【請求項１】　通信網によって相互に接続された複数の端末からなり、複数の端末を中継してデータを通信する通信システムにおいて、

送信者と受信者の間で通信される通信データが途中通信経路の検閲端末で検閲処理が行われる環境にある場合、前記検閲端末が行う検閲処理により送信者の送信した通信データを検閲し、検閲された通信データと検閲前の通信データを前記検閲端末のデジタル署名とともに送信元に返送するステップと、

検閲を受けた通信データの返送を受けた送信者のデジタル署名プロセスが、検閲前の通信データと検閲された通信データとを比較し、検閲された通信内容に対してデジタル署名を行い、検閲端末を介して、受信者に転送するステップとからなり、

検閲端末から受信した通信データの受信者が、受信した通信内データとデジタル署名からデータの一貫性が確認できることを特徴とするデータ保証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークを介してデータの交換を行うデータ転送システムに関わり、特に、転送されたデータの完全性を保証するデータ転送システムに関するものである。ここで、データの完全性とは、送信者の送信したデータと受信者の受信したデータが完全に一致することをいう。

【０００２】

【従来の技術】ネットワークを介し、データの交換を行うデータ転送システムにおいて、転送されているデータの全部もしくは一部が、途中経路で変更・削除されることは、安全上の重大な問題となる。そこで、現在は一方向性関数と公開鍵暗号から作られるデジタル署名を利用することによって、安全性を確保し、盗聴、秘密の漏洩などの問題が、発生しないようにしている。

【０００３】この技術について、図１、図２および図３を用いて説明する。

【０００４】具体的に、図１に示すように送信者１０１と受信者１０２が一方向性関数アルゴリズム１０３と公開鍵暗号アルゴリズム１０４と送信者の公開鍵１０５を共有しており、送信者１０１は自分の個人鍵１０７を保持している状況で、送信者１０１の持っている通信内容１０６を受信者１０２に通信する場合を図２の流れ図に従って説明する。

【０００５】ここで、一方向性関数とは、任意の長さの入力データに対して、固定長の出力データを算出し、同じ入力データに対しては同じ出力データを算出し、出力データから入力データを推測することが非常に困難であるような特徴を持った関数である。

【０００６】また、個人鍵とは、公開鍵暗号で任意の受信者に割り当てられる２つの鍵のうちの１つを示している。

2

【０００７】公開鍵暗号とは、暗号化と復号で異なる鍵を利用する暗号方式であり、情報の受信者に、公開鍵と呼ばれる鍵と対応する個人鍵と呼ばれる鍵をペアで割り当てて、公開鍵を公に公開し、個人鍵を秘密に保持している状況で、情報を送りたい送信者が、受信者の公開鍵でその情報を暗号化することで、安全に受信者に送ることができる仕組みを提供するものである。

【０００８】この技術は、公開鍵で暗号化した情報は、対応する個人鍵でしか復号できない性質を利用して実現されているからである。さらに、公開鍵暗号は、個人鍵で暗号化した情報も、対応する公開鍵でしか復号できないので、送信者が自分の個人鍵で情報を暗号化して、それを受信者が送信者の公開鍵で復号すれば、送信者の認証としても利用することができる。

【０００９】図２において、まず、送信者１０１は送信する通信内容１０６を入力として一方向性関数アルゴリズム１０３の出力であるハッシュ値を算出する（ステップ２０１）。次に送信者１０１は、ステップ２０１で算出したハッシュ値を送信者１０１の個人鍵１０７と公開鍵暗号アルゴリズム１０４で暗号化する。これをデジタル署名と呼ぶ（ステップ２０２）。デジタル署名の例を図３に示す。

【００１０】次に、送信者１０１は通信内容１０６とステップ２０２で作成したデジタル署名を受信者１０２に送信する（ステップ２０３）。

【００１１】次に、受信者１０２はステップ２０３で送信された通信内容１０６とデジタル署名ををを受信する（ステップ２０４）。

【００１２】次に、受信者１０２はステップ２０４で受信した通信内容１０６を入力として一方向性関数アルゴリズム１０３の出力であるハッシュ値を算出する（ステップ２０５）。

【００１３】次に、ステップ２０４で受信したデジタル署名を送信者１０１の公開鍵暗号アルゴリズム１０４と公開鍵１０５で復号する（ステップ２０６）。次に、受信者１０２は、ステップ２０５で算出したハッシュ値とステップ２０６で復号したデジタル署名を比較する。同一データであれば、ステップ２０８へ進み、異なったデータであれば、ステップ２１０へ進む（ステップ２０７）。送信者１０２は通信内容が改ざんされていなかったと判断する（ステップ２０８）。

【００１４】送信者１０２は通信内容が改ざんされていると判断する（ステップ２１０）。

【００１５】なお、ステップ２０２で開示されるデジタル署名については例えば、図８に示す通信内容に対して、一方向性関数アルゴリズムとしてＲＦＣ１３２１で規定されているＭＤ５を利用し、公開鍵暗号アルゴリズムとしてＲＳＡ暗号を利用した場合のデジタル署名を図３に示す。

【００１６】こうした方法は、インターネットの標準プロトコルとしてＲＦＣ１４２１～ＲＦＣ１４２４に記述されている暗号電子メールシステムＰＥＭ（Ｐｖａｃｙ Ｅｎｈａｎｃｅｄ Ｍａｉｌ）やＰｈｉｌｉｐ Ｒ．Ｚｉｍｍｅｒｍａｎｎにより開発されたＰＧＰ（Ｐｒｉｔｙ Ｇｏｏｄ Ｐｒｉｖａｃｙ）の中に取り入れられている。

【００１７】

【発明が解決しようとする課題】ところで、最近、インターネットの普及により、コンピュータネットワーク上で、青少年に害をなす猥褻な画像などの有害情報が閲覧可能になってしまっている。そこで政府やネットワークプロバイダが市民やユーザに有害な情報を提供しないように、通信内容の検閲を行っている。

【００１８】この技術は、通信内容を提供するマシンへのアクセス権や通信内容全体の閲覧権を設定する方法で行われている。

【００１９】しかし、従来の技術では、検閲者もしくは、検閲プロセスが受信者に暴力的イメージや性的表現などの有害な情報を与えないために、通信経路の途中で通信内容を検閲して、通信内容の一部を削除した場合に、通信内容の最終的な受信者は、チェックデータを計算できず、送信者の保証したデータの完全性を確かめることができない。

【００２０】本発明の目的は、故意、悪意により通信内容の一部が削除されるような検閲を受けた場合でも、送信者の保証したデータの完全性を確保できるシステムを提案することにある。

【００２１】

【課題を解決するための手段】この課題を解決するために、本システムでは、検閲者もしくは、検閲プロセスが削除・変更した通信内容を送信者に戻して新たに通信内容の完全性を保証するデジタル署名を計算することを提案している。この時、送信者が常に返送される変更・修正された通信内容を監視する必要は無く、自動的にデジタル署名を行い、受信者に再送信される。

【００２２】

【発明の実施の形態】以下、本発明の実施形態の例を図面を用いて詳細に説明する。なお、同一番号は同様の部品・要素を表す。

【００２３】図４において、４０１、４０２、４０３はそれぞれ送信者、検閲者、受信者であり、４０４、４０５、４０６は送信者、検閲者、受信者、認証者のワークステーションである。

【００２４】ワークステーション４０４とワークステーション４０５は通信網４０７を介して相互に通信を行うことができ、ワークステーション４０５とワークステーション４０６は通信網４０８を介して相互に通信を行うことができる。そして、ワークステーション４０５とワークステーション４０７は、通信網４０７とワークステーション４０５と通信網４０８を介して通信を行うことができる。送信者４０１や受信者４０２、検閲者４０３は、ユーザ、あるいは、プログラムを示している。

【００２５】図５に示す送信者４０１のワークステーション４０４は、通信網との間でデータのやりとりを行う通信網インターフェース５０１と、ユーザにメッセージ等を表示するディスプレイ５０２と、ユーザがデータ等を入力するためのキーボード５０３と、演算処理を行うＣＰＵ５０４とメモリ５０５、通信プログラム５０６やデジタル署名作成プログラム５０７やデジタル署名検証プログラム５０８やデータ比較プログラム５０９や認証局の公開鍵５１０や通信内容５１１や履歴テーブル５１２やデジタル署名作成用の設定パラメータテーブル５１４が記録されている外部記憶装置５１３とを有しており、それらはバス５００によって相互に接続されている。

【００２６】ここで、認証局は任意の公開鍵の正当な所有者を承認して、その公開鍵にデジタル署名を発行する機関であることを示す。

【００２７】図６は、設定パラメータテーブル５１６の構造を示したものである。６００には利用可能な一方向性関数アルゴリズム識別子がつけられている。６０１には利用可能な公開鍵暗号アルゴリズム識別子がつけられている。６０２にはそのアルゴリズムに対応した送信者４０１の個人鍵がつけられている。６０３には対応した送信者４０１の公開鍵がつけられている。１００４は６０３の公開鍵について認証局が発行したデジタル署名が格納されている。

【００２８】図７は、履歴テーブル５１２の構造を示したものである。７０１は検閲前の通信内容、７０２は通信内容７０１のデジタル署名、７０３は一方向性関数アルゴリズム識別子、７０４は公開鍵暗号アルゴリズム識別子、７０５には検閲された通信内容、７０６は通信内容７０５のデジタル署名、７０７はデジタル署名７０６を施した署名者の名前、７０８には通信内容７０５を復号するための公開鍵が格納されている。

【００２９】外部記憶装置５１３に記憶されている通信プログラム５０６は、他の端末との間でデータのやりとりを行う場合にその制御を行うプログラムである。

【００３０】デジタル署名作成プログラム５０７は、プログラムに与えられた通信内容が改ざんされていないことを保証し、送信者を正しく識別できるデジタル署名を作成するプログラムである。

【００３１】図９は、ワークステーション４０４～６間で通信するデータの構造を示している。９０１はデータ構造全体を表し、通信データと呼ぶ。通信データ９０１は本来、通信相手に伝えたい内容を示す通信内容９０２と主署名者パラメータ部９１２と副署名者パラメータ部９１３に分けることができる。

【００３２】主署名者パラメータ部９１２は、メインの

デジタル署名者による通信内容の完全性を検証するためにデジタル署名９０３とデジタル署名を施した署名者名９０４、署名者の公開鍵９０５と署名者の公開鍵９０５に対する認証局のデジタル署名９０６、採用した一方向性関数アルゴリズム識別子９０９と公開鍵暗号アルゴリズム識別子９１０で構成されている。

【００３３】副署名者パラメータ部９１３は、メインとは別のデジタル署名者による通信内容に対するデジタル署名９０７や署名を施したデジタル署名者名９０８を追加することができる。また、通信データ９０１は副署名者パラメータ部９１３を複数持つことができる。

【００３４】デジタル署名検証プログラム５０８は、プログラムに与えられた通信データの通信内容とデジタル署名を比較して、通信内容の改ざんや送信者の正しい識別ができたことを確認するプログラムである。

【００３５】データ比較プログラム５０９は、プログラムに与えられた検閲前の通信内容と検閲後の通信内容を比較して、検閲後の通信内容が検閲前の通信内容を削除して作られたものであることを確認するプログラムである。

【００３６】図１０に示す検閲者４０２のワークステーション４０５は、通信網との間でデータのやりとりを行う通信網インターフェース５０１と、ユーザにメッセージ等を表示するディスプレイ５０２と、ユーザがデータ等を入力するためのキーボード５０３と、演算処理を行うＣＰＵ５０４とメモリ５０５、通信プログラム５０６やデジタル署名作成プログラム５０７やデジタル署名検証プログラム５０８や検閲プログラム１１０１や認証局の公開鍵５１０やデジタル署名作成用の設定パラメータテーブル５１４や検閲する言葉の格納してある検閲ワードテーブル１１０２が記録されている外部記憶装置５１３とを有しており、それらはバス５００によって相互に接続されている。

【００３７】図１１は検閲ワードテーブル１１０２の例を示す図である。検閲ワードテーブル１１０２は検閲者のポリシが反映されており、例えば、外部に開示したくない組織内のサブ組織名や製品のコードネームや露骨でひわいな表現や相手を侮辱する表現などが格納されている。

【００３８】検閲プログラム１１０１は、プログラムに与えられた通信内容に検閲ワードテーブルに格納されている表現があるか検索して、もしあった場合に、通信内容からその表現を削除するプログラムである。

【００３９】図１２に示す受信者４０３のワークステーション４０６は、通信網との間でデータのやりとりを行う通信網インターフェース５０１と、ユーザにメッセージ等を表示するディスプレイ５０２と、ユーザがデータ等を入力するためのキーボード５０３と、演算処理を行うＣＰＵ５０４とメモリ５０５、通信プログラム５０６やデジタル署名作成プログラム５０７やデジタル署名検証プログラム５０８や認証局の公開鍵５１０やデジタル署名作成用の設定パラメータテーブル５１４が記録されている外部記憶装置５１３とを有しており、それらはバス５００によって相互に接続されている。

【００４０】図１３を用いて、通信データが送信者で作成されてから受信者に受理されるまでの手順を説明する。

【００４１】まず、送信者４０１は通信内容５１１のデータの完全性を保証するデジタル署名方式をワークステーション４０４の外部記憶装置５１３にあるデジタル署名作成用の設定パラメータテーブル５１４から選択する（ステップ１３０１）。

【００４２】次に、送信者４０１はワークステーション４０４の外部記憶装置５１３にあるデジタル署名作成プログラム５０７に通信内容５１１とステップ１４０１で選択したデジタル署名作成用の設定パラメータを与えて、ワークステーション４０４のメモリ５０５上で実行させ、通信内容５１１に対する送信者４０１のデジタル署名を算出する（ステップ１３０２）。図８に通信内容の例を示し、図３にその通信内容に対するデジタル署名を示す。

【００４３】次に、送信者４０１は通信内容５１１とステップ１３０１で選択された設定パラメータとステップ１３０２で算出されたデジタル署名から、図９に示したデータ構造の通信データを作成して、送信する（ステップ１３０３）。

【００４４】次に、検閲者４０２がステップ１３０３で送信者４０１により作成・送信された通信データを受信する（ステップ１３０４）。

【００４５】次に、検閲者４０２はステップ１３０４で受信した通信データの複数あるデジタル署名者名に検閲者４０２自身の名前がないかどうか確認する。あった場合はステップ１３１６へ進む。なかった場合は、ステップ１３０６へ進む（ステップ１３０５）。

【００４６】次に、検閲者４０２はワークステーション４０５の外部記憶装置５１３にあるデジタル署名検証プログラム５０８に、ステップ１３０４で受信した通信データを与えて、ワークステーション４０５のメモリ５０５上で実行させ、通信データ内の通信内容が改ざんされていないか確認する。改ざんされていればステップ１３２１へ進む。改ざんされていなければステップ１３０７へ進む（ステップ１３０６）。

【００４７】次に、検閲者４０２はワークステーション４０５の外部記憶装置５１３にある検閲プログラム１１０１に、ステップ１３０６で改ざんされていないこと確認された通信内容を与えて、ワークステーション４０５のメモリ５０５上で実行させて、検閲後の通信内容を得る。ここで、通信内容の検閲は、検閲プログラム１１０１で行わないで、人間である検閲者が手動で行う場合も想定している（ステップ１３０７）。

【００４８】次に、検閲者４０２はワークステーション４０５の外部記憶装置５１３にあるデジタル署名作成プログラム５０７にステップ１３０４で受信した通信データ内に含まれる一方向性関数アルゴリズム識別子と公開鍵暗号アルゴリズム識別子で一意に決定できるワークステーション４０５のデジタル署名作成用の設定パラメータテーブル５１４上の設定パラメータを与えて、ワークステーション４０５のメモリ５０５上で実行させ、ステップ１３０７で検閲した通信内容に対する検閲者４０２のデジタル署名を算出する（ステップ１３０８）。

【００４９】次に、検閲者４０２はステップ１３０７で検閲した通信内容とステップ１３０８で選択された設定パラメータとステップ１３０８で算出されたデジタル署名から、図９に示したデータ構造の通信データを作成し、さらに、ステップ１３０４で受信した通信データを連結して、送信者４０１に送信する（ステップ１３０９）。

【００５０】次に、送信者４０１はステップ１３０９で検閲者４０２により作成・送信された連結された２つの通信データを受信する（ステップ１３１０）。

【００５１】次に、送信者４０１はワークステーション４０４の外部記憶装置５１３にあるデジタル署名検証プログラム５０８に、ステップ１３１０で受信した２つの通信データをそれぞれ個別に与えて、ワークステーション４０４のメモリ５０５上で実行させ、通信データ内の通信内容が改ざんされていないか確認する。どちら一方の通信内容が改ざんされていればステップ１３２１へ進む。どちらも改ざんされていなければステップ１３１２へ進む（ステップ１３１１）。

【００５２】次に、送信者４０１はワークステーション４０４の外部記憶装置５１３にあるデータ比較プログラム５０９に、ステップ１３１１で検証した検閲前の通信内容と検閲後の通信内容を与えて、ワークステーション４０４のメモリ５０５上で実行させ、検閲後の通信内容が検閲前の通信内容を削除しただけのものであることを確認する。検閲後の通信内容が削除しただけのものであればステップ１３１３へ進む。それ以外はステップ１３２１へ進む（ステップ１３１２）。

【００５３】次に、送信者４０１はステップ１３１０で受信した２つの通信データのコピーをを外部記憶装置５１３の履歴テーブルに格納する（ステップ１３１３）。

【００５４】次に、送信者４０１はワークステーション４０４の外部記憶装置５１３にあるデジタル署名作成プログラム５０７にステップ１３１０で受信した通信データ内に含まれる一方向性関数アルゴリズム識別子と公開鍵暗号アルゴリズム識別子で一意に決定できるワークステーション４０４のデジタル署名作成用の設定パラメータテーブル５１４上の設定パラメータを与えて、ワークステーション４０４のメモリ５０５上で実行させ、ステップ１３１２で確認した検閲後の通信内容に対する送信者４０１のデジタル署名を算出する（ステップ１３１４）。

【００５５】次に、送信者４０１はステップ１３１２で確認した検閲後の通信内容とステップ１３１４で選択された設定パラメータとステップ１３１４で算出されたデジタル署名から、図９に示したデータ構造の通信データを作成して、送信する（ステップ１３１５）。こうして、ステップ１３０４に戻る。

【００５６】次に、ステップ１３０５で検閲者４０２のデジタル署名があった場合の処理を以下に示す。

【００５７】検閲者４０２はワークステーション４０５の外部記憶装置５１３にあるデジタル署名検証プログラム５０８に、ステップ１３０４で受信した通信データを与えて、ワークステーション４０５のメモリ５０５上で実行させ、通信データ内の通信内容が改ざんされていないか確認する。改ざんされていればステップ１３２１へ進む。改ざんされていなければステップ１３１７へ進む（ステップ１３１６）。

【００５８】次に、検閲者４０２はステップ１３１６で改ざんされていないことを確認された通信データを受信者４０３に向けて転送する（ステップ１３１７）。

【００５９】次に、受信者４０３がステップ１３１７で検閲者４０２により転送された通信データを受信する（ステップ１３１８）。

【００６０】次に、受信者４０３はワークステーション４０６の外部記憶装置５１３にあるデジタル署名検証プログラム５０８に、ステップ１３１８で受信した通信データを与えて、ワークステーション４０６のメモリ５０５上で実行させ、通信データ内の通信内容が改ざんされていないか確認する。改ざんされていればステップ１３２１へ進む。改ざんされていなければステップ１３２０へ進む（ステップ１３１９）。

【００６１】次に、受信者４０３は、ステップ１３１９でデータの完全性が確認された通信内容を受理する（ステップ１３２０）。

【００６２】最後に、ステップ１３０６、１３１１、１３１２、１３１６、１３１９で通信内容に改ざんがあった場合の処理を示す。

【００６３】改ざんをあった場合、送信者４０1、検閲者４０２、受信者４０３、いづれの場合も通信データを全て消去する（ステップ１３２１）。

【００６４】デジタル署名作成プログラム５０７の動作手順を図１４の流れ図で説明する。

【００６５】与えられた通信内容を入力として、与えられたデジタル署名用の設定パラメータで指定された一方向性関数アルゴリズムでハッシュ値を算出する（ステップ１４０１）。

【００６６】与えられたデジタル署名用の設定パラメータで指定された公開鍵暗号アルゴリズムと対応する個人鍵で、ステップ１４０１算出したハッシュ値を暗号化し

て、デジタル署名を算出する（ステップ１４０２）。

【００６７】デジタル署名検証プログラム５０８の動作手順を図１５の流れ図で説明する。

【００６８】与えられた通信データの主署名者パラメータ部にある署名者の公開鍵のデジタル署名を取り出し、主署名者パラメータ部の公開鍵暗号アルゴリズム識別子で指定される公開鍵暗号アルゴリズムと外部記憶装置に５１３にある認証局の公開鍵５１０で復号する（ステップ１５０１）。与えられた通信データの主署名者パラメータ部にある署名者の公開鍵を入力として、主署名者パラメータ部の一方向性関数アルゴリズム識別子で指定される一方向性関数アルゴリズムでハッシュ値を算出する（ステップ１５０２）。

【００６９】ステップ１５０１で復号したデジタル署名とステップ１５０２で算出したハッシュ値を比較する。同じデータであれば、ステップ１５０４へ進む。異なったデータであればステップ１５１０へ進む（ステップ１５０３）。

【００７０】与えれられた通信データの主署名者パラメータ部にある通信内容のデジタル署名を通信データの主署名者パラメータ部にある公開鍵暗号アルゴリズム識別子で指定される公開鍵暗号アルゴリズムと通信データの主署名者パラメータ部にある公開鍵で復号する（ステップ１５０４）。与えられた通信データの通信内容を入力として、主署名者パラメータ部の一方向性関数アルゴリズム識別子で指定される一方向性関数アルゴリズムでハッシュ値を算出する（ステップ１５０５）。

【００７１】ステップ１５０４で復号したデジタル署名とステップ１５０５で算出したハッシュ値を比較する。同じデータであれば、ステップ１５０７へ進む。異なったデータであればステップ１５１０へ進む（ステップ１５０６）。通信データの通信内容が改ざんされていなかったことと判断する（ステップ１５０７）。通信データの通信内容が改ざんされていると判断する（ステップ１５１０）。

【００７２】データ比較プログラム５０８の動作手順を図１６の流れ図で説明する。

【００７３】最初に変数Ｉに「１」をセットする（ステップ１６０１）。与えられた検閲前の通信内容の先頭からＩ番目の文字データを取り出す（ステップ１６０２）。

【００７４】同様に、与えられた検閲後の通信内容の先頭からＩ番目の文字ータを取り出す（ステップ１６０３）。次に、ステップ１６０２とステップ１６０３で文字が取り出せたか確認する。ステップ１６０２とステップ１６０３の両方で文字データが取り出せれば、ステップ１６０５へ進む。逆に、ステップ１６０２とステップ１６０３の両方で文字データが取り出せなければ、ステップ１６１０へ。それ以外は、ステップ１６１１へ進む（ステップ１６０４）。

【００７５】ステップ１６０３で得られた文字が、検閲文字であるならステップ１６０７へ。そうでなけば、ステップ１６０６へ進む。ここで、検索文字とは「■」を表す（ステップ１６０５）。

【００７６】次に、ステップ１６０２で得られた文字とステップ１６０３で得られた文字を比較する。同じ文字データでならば、ステップ１６０７へ進む。異なった文字データであればステップ１６１１へ進む（ステップ１６０６）。

【００７７】次に、変数Ｉの値を「１」増やし、ステップ１６０２に戻る（ステップ１６０７）。通信データの通信内容が改ざんされていなかったと判断する（ステップ１６１０）。通信データの通信内容が改ざんされていると判断する（ステップ１６１１）。

【００７８】検閲プログラム１１０１の動作手順を図１７の流れ図で説明する。

【００７９】変数Ｉに「１」をセットする（ステップ１７０１）。外部記憶装置５１３にある検閲ワードテーブル１１０２のＩ番目のワードデータを取り出す。ワードが取り出せれば、ステップ１７０３へ進む。取り出せなければ、終了する（ステップ１７０２）。

【００８０】ステップ１７０２で取り出したワードデータをキーに与えられた通信内容を検索する。検索がマッチすればステップ１７０４へ、通信内容を最後まで検索したらステップ１７０５へ進む（ステップ１７０３）。通信内容の検索がマッチしたワードの全文字をを検閲文字に置き換える。そして、ステップ１７０３へ戻る（ステップ１７０４）。

【００８１】次に、変数Ｉの値を「１」増やし、ステップ１８０２に戻る（ステップ１７０５）。

【００８２】

【発明の効果】本発明により、以下の示す２つの効果が得られる。

【００８３】１）検閲により通信内容の変更があった場合でも通信内容の最終的な受信者がデータの完全性をチェックできる。

【００８４】２）通信内容の検閲の履歴を送信者が全て記録できるので、検閲者もしくは、検閲プロセスが複数いた時にどの検閲者もしくは、検閲プロセスがどの部分を削除したか判別することができる。

【図面の簡単な説明】

【図１】デジタル署名による認証方法で必要な要素を示す構成図である。

【図２】デジタル署名による認証方法の処理手順を示す流れ図である。

【図３】図８の通信内容に対するデジタル署名を示した図である。

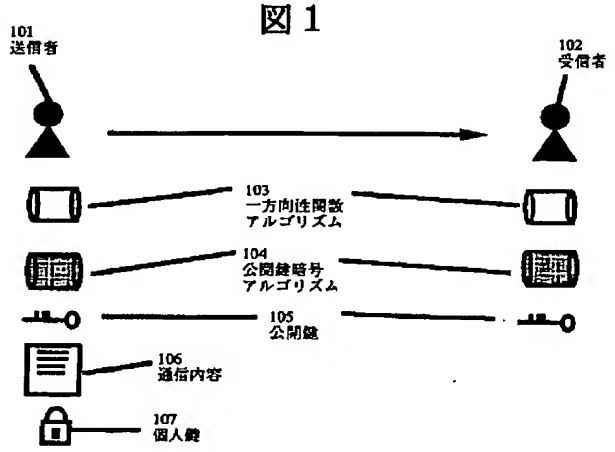
【図４】本発明の実施形態の基本構成を示すシステム構成図である。

【図５】送信者のワークステーションの基本構成を示す

システム構成図である。
【図６】デジタル署名用の設定パラメータを格納するテーブルの構成図である。
【図７】履歴情報を格納するテーブルの構成図である。
【図８】通信内容の例を示した図である。
【図９】ワークステーション間で通信される情報のデータ構造を示した構成図である。
【図１０】検閲者のワークステーションの基本構成図を示すシステム構成図である。
【図１１】検閲ワードを格納するテーブルの構成図である。
【図１２】受信者のワークステーションの基本構成を示すシステム構成図である。
＊【図１３】本発明の実例の基本的な処理手順を示す流れ図である。
【図１４】デジタル署名作成プログラムの処理手順を示す流れ図である。
【図１５】デジタル署名検証プログラムの処理手順を示す流れ図である。
【図１６】データ比較プログラムの処理手順を示す流れ図である。
【図１７】検閲プログラムの処理手順を示す流れ図である。
【符号の説明】
４０１…送信者、４０２…検閲者、４０３…受信者、４０４…ワークステーション。

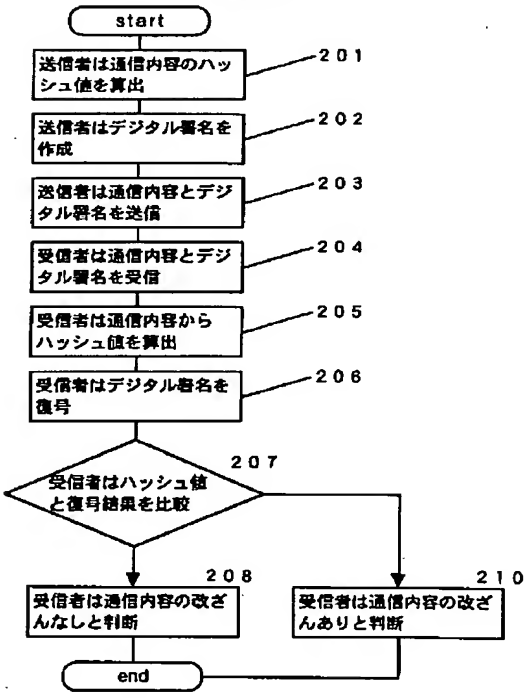
【図１】

図１



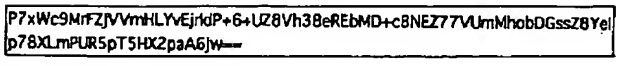
【図２】

図２



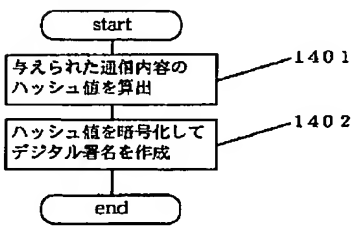
【図３】

図３



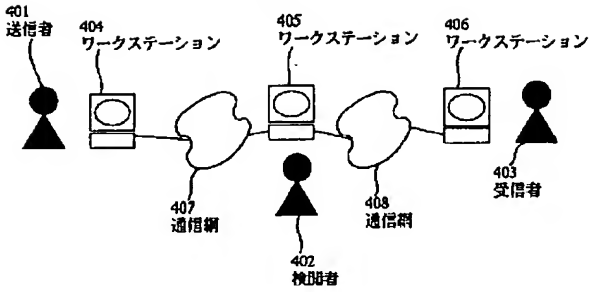
【図１４】

図１４



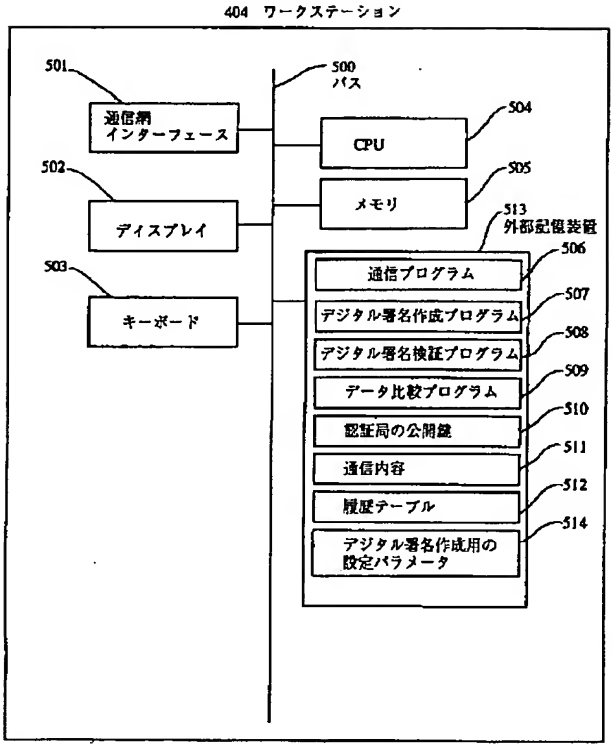
【図4】

図4



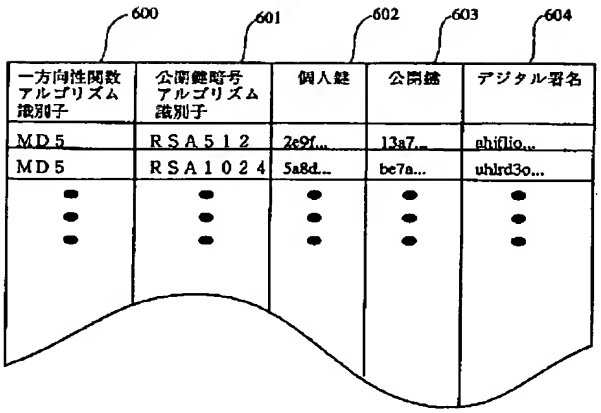
【図5】

図5



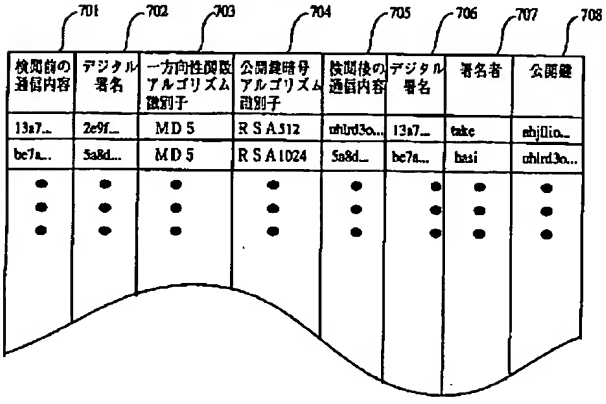
【図6】

図6



【図7】

図7



【図８】

図８

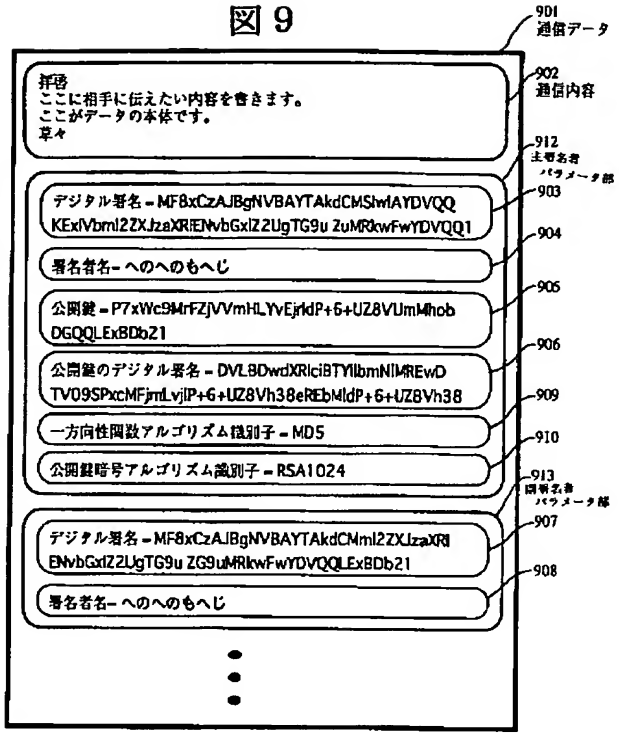
```
bonsai% hping
PING hskgw.hitachi-sk.co.jp: 56 data bytes
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=0. time=685. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=1. time=590. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=2. time=480. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=3. time=699. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=4. time=589. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=5. time=900. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=6. time=648. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=7. time=973. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=8. time=917. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=9. time=614. ms

----2.1.107.133.in-addr.arpa PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 480/709/973

△山○男
```

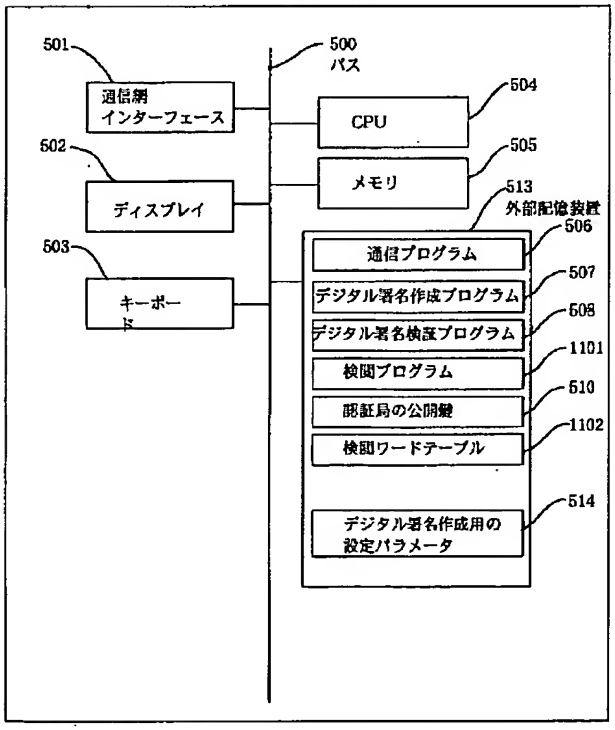
【図９】

図９



【図１０】

図１０



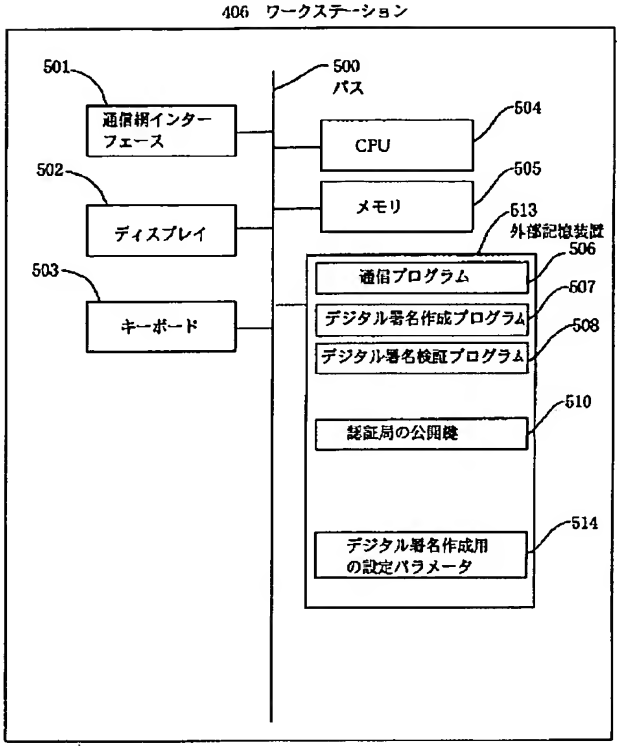
【図１１】

図１１

#	ワードデータ
1	携帯端末課
2	Windows NT課
●	●
●	●
●	●

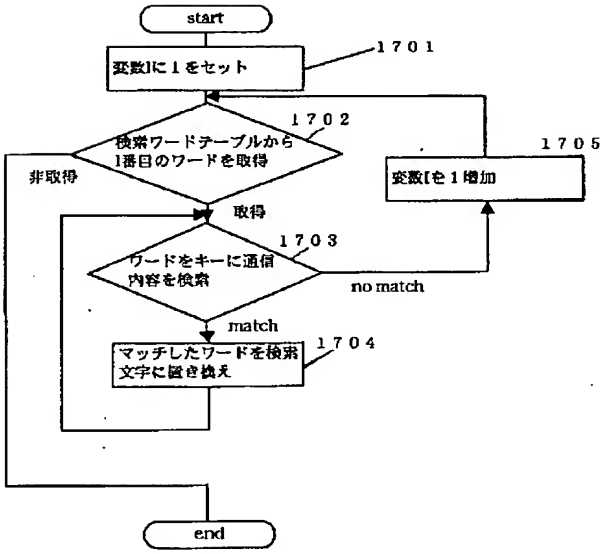
【図１２】

図１２



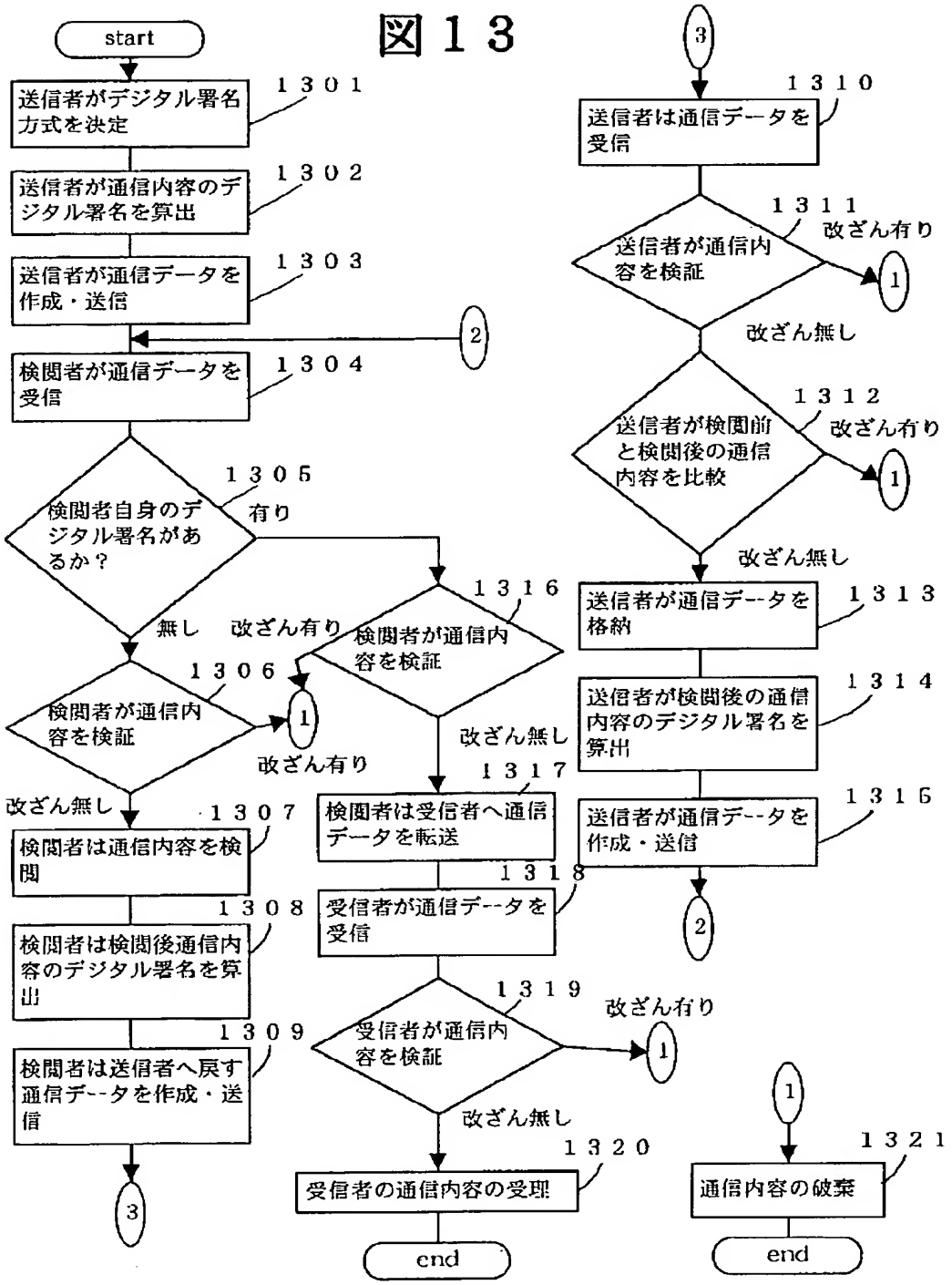
【図１７】

図１７



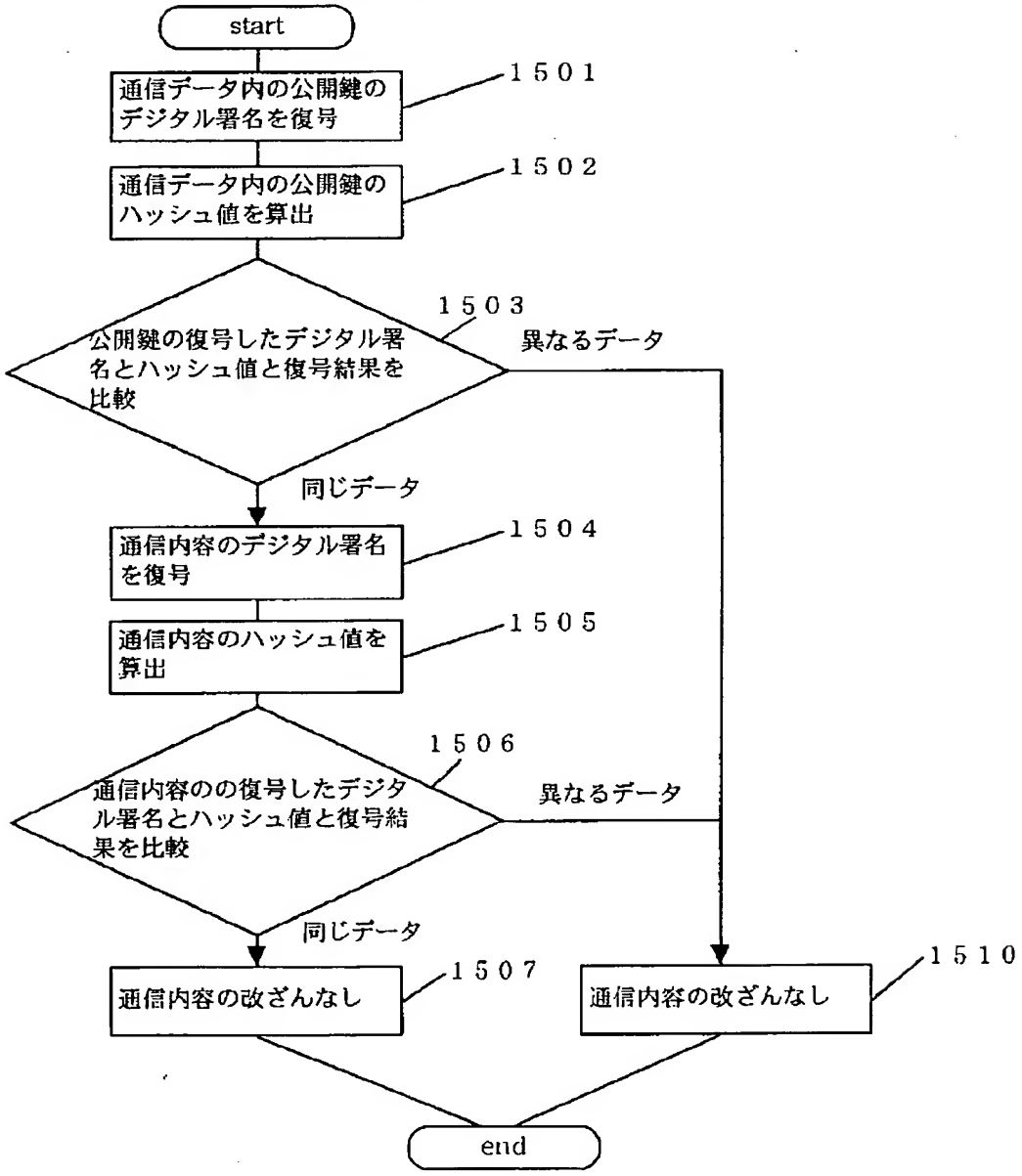
【図１３】

図１３


start
送信者がデジタル署名方式を決定
１３０１
送信者が通信内容のデジタル署名を算出
１３０２
送信者が通信データを作成・送信
１３０３
検閲者が通信データを受信
１３０４
検閲者自身のデジタル署名があるか？
１３０５
有り
無し
改ざん有り
検閲者が通信内容を検証
１３０６
改ざん有り
改ざん無し
検閲者は通信内容を検閲
１３０７
検閲者は検閲後通信内容のデジタル署名を算出
１３０８
検閲者は送信者へ戻す通信データを作成・送信
１３０９
検閲者が通信内容を検証
１３１６
改ざん有り
改ざん無し
検閲者は受信者へ通信データを転送
１３１７
受信者が通信データを受信
１３１８
受信者が通信内容を検証
１３１９
改ざん有り
改ざん無し
受信者の通信内容の受理
１３２０
end
送信者は通信データを受信
１３１０
送信者が通信内容を検証
１３１１
改ざん有り
改ざん無し
送信者が検閲前と検閲後の通信内容を比較
１３１２
改ざん有り
改ざん無し
送信者が通信データを格納
１３１３
送信者が検閲後の通信内容のデジタル署名を算出
１３１４
送信者が通信データを作成・送信
１３１６
通信内容の破棄
１３２１
end
1
2
3

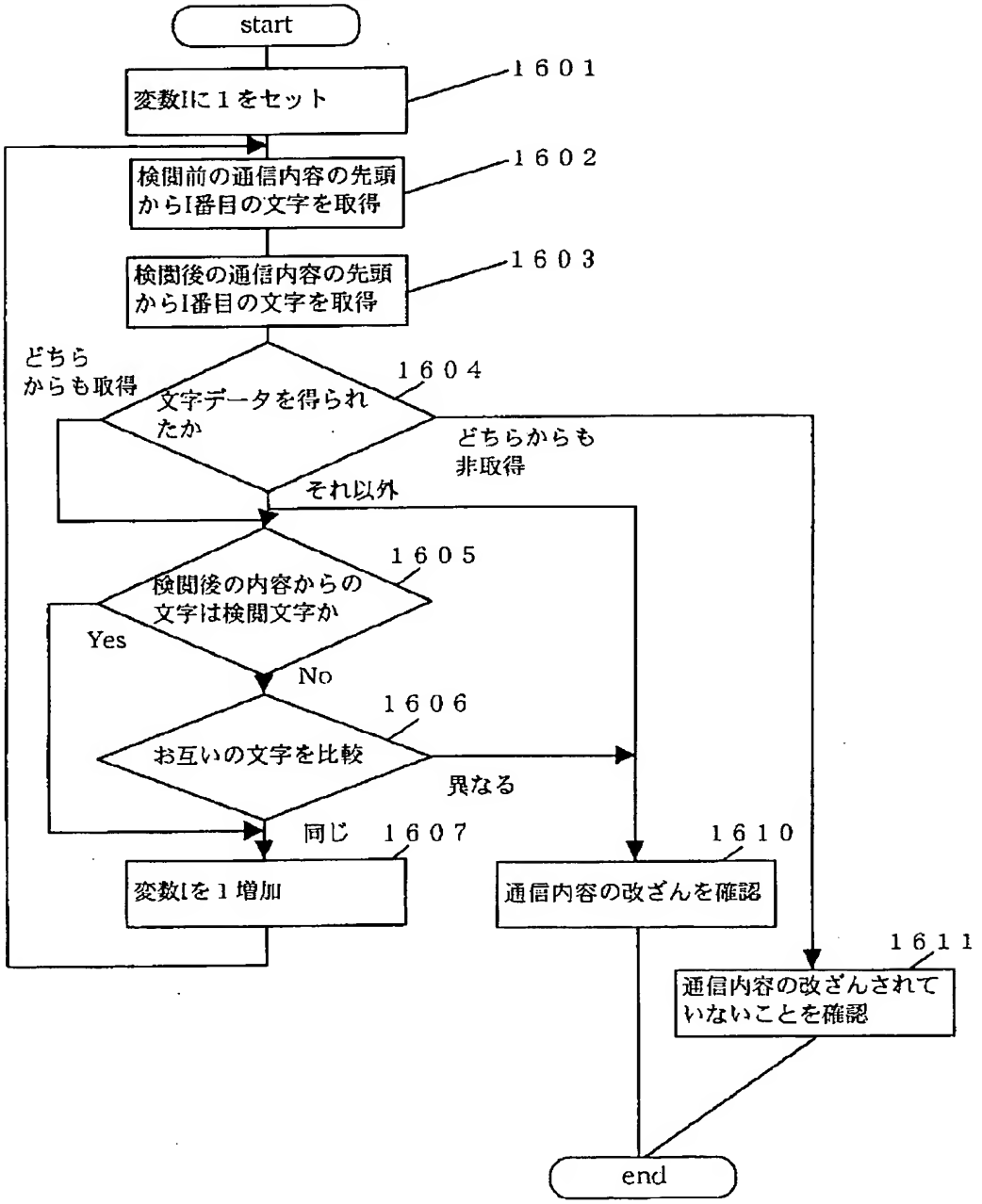
【図１５】

図１５


start
通信データ内の公開鍵のデジタル署名を復号
１５０１
通信データ内の公開鍵のハッシュ値を算出
１５０２
公開鍵の復号したデジタル署名とハッシュ値と復号結果を比較
１５０３
異なるデータ
同じデータ
通信内容のデジタル署名を復号
１５０４
通信内容のハッシュ値を算出
１５０５
通信内容のの復号したデジタル署名とハッシュ値と復号結果を比較
１５０６
異なるデータ
同じデータ
通信内容の改ざんなし
１５０７
通信内容の改ざんなし
１５１０
end

【図１６】

図１６


start
変数Iに１をセット
１６０１
検閲前の通信内容の先頭からI番目の文字を取得
１６０２
検閲後の通信内容の先頭からI番目の文字を取得
１６０３
どちらからも取得
文字データを得られたか
１６０４
どちらからも非取得
それ以外
検閲後の内容からの文字は検閲文字か
１６０５
Yes
No
お互いの文字を比較
１６０６
異なる
同じ
１６０７
変数Iを１増加
１６１０
通信内容の改ざんを確認
１６１１
通信内容の改ざんされていないことを確認
end

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成１４年1月２３日（２００２．１．２３）

【公開番号】特開平１０－１０５０５８
【公開日】平成１０年４月２４日（１９９８．４．２４）
【年通号数】公開特許公報１０－１０５１
【出願番号】特願平８－２５４０５７
【国際特許分類第７版】
G09C 1/00 640

【ＦＩ】
G09C 1/00 640 Z
640 D
640 E

【手続補正書】
【提出日】平成１３年６月１２日（２００１．６．１２）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正内容】
【発明の名称】　データ保証システムおよびデータ保証方法
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　通信網によって相互に接続された複数の端末からなり、送信者と受信者との間で通信される通信データが通信経路間の検閲端末により検閲処理されるデータ保証システムであって、
前記検閲端末は、送信元の端末から送信された通信データを検閲する手段と、
検閲後の通信データと検閲前の通信データとを、前記検閲端末のデジタル署名とともに送信元の端末に返送する手段とを有し、
前記送信元の端末は、前記検閲後の通信データが返送されてきた場合に、前記検閲前の通信データと、前記検閲後の通信データとを比較して通信データの改ざんがないかを検証し、改ざんがない場合に、前記検閲後の通信データに対してデジタル署名を行う手段と、
前記検閲端末を介して、前記検閲後の通信データを受信先の端末に送信する手段とを有することを特徴とするデータ保証システム。

【請求項２】　通信網によって相互に接続された複数の端末からなり、送信者と受信者との間で通信される通信データが通信経路間の検閲端末により検閲処理されるデータ保証システムにおけるデータ保証方法であって、
前記検閲端末において、送信元の端末から送信された通信データを検閲し、検閲後の通信データと検閲前の通信データとを、前記検閲端末のデジタル署名とともに送信元の端末に返送し、
前記送信元の端末において、前記検閲後の通信データが返送されてきた場合に、前記検閲前の通信データと、前記検閲後の通信データとを比較して通信データの改ざんがないかを検証し、改ざんがない場合に、前記検閲後の通信データに対してデジタル署名を行い、前記検閲端末を介して、前記検閲後の通信データを受信先の端末に送信することを特徴とするデータ保証方法。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正内容】
【００１１】次に、受信者１０２はステップ２０３で送信された通信内容１０６とデジタル署名を受信する（ステップ２０４）。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】変更
【補正内容】
【００２１】
【課題を解決するための手段】この課題を解決するために、本システムでは、検閲者もしくは、検閲プロセスが削除・変更した通信内容を送信者に戻して新たに通信内

容の完全性を保証するデジタル署名を計算することを提案する。この時、送信者が常に返送される変更・修正された通信内容を監視する必要は無く、自動的にデジタル署名を行い、受信者に再送信される。即ち、本発明は、通信網によって相互に接続された複数の端末からなり、送信者と受信者との間で通信される通信データが通信経路間の検閲端末により検閲処理されるデータ保証システムにおいて、前記検閲端末において、送信元の端末から送信された通信データを検閲し、検閲後の通信データと検閲前の通信データとを、前記検閲端末のデジタル署名とともに送信元の端末に返送し、前記送信元の端末において、前記検閲後の通信データが返送されてきた場合に、前記検閲前の通信データと、前記検閲後の通信データとを比較して通信データの改ざんがないかを検証し、改ざんがない場合に、前記検閲後の通信データに対してデジタル署名を行い、前記検閲端末を介して、前記検閲後の通信データを受信先の端末に送信することを特徴とする。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００２４
【補正方法】変更
【補正内容】
【００２４】ワークステーション４０４とワークステーション４０５は通信網４０７を介して相互に通信を行うことができ、ワークステーション４０５とワークステーション４０６は通信網４０８を介して相互に通信を行うことができる。そして、ワークステーション４０４とワークステーション４０６は、通信網４０７とワークステーション４０５と通信網４０８を介して通信を行うことができる。送信者４０１や検閲者４０２、受信者４０３は、ユーザ、あるいは、プログラムを示している。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００３７
【補正方法】変更
【補正内容】
【００３７】図１１は検閲ワードテーブル１１０２の例を示す図である。検閲ワードテーブル１１０２は検閲者のポリシーが反映されており、例えば、外部に開示したくない組織内のサブ組織名や製品のコードネームや露骨でひわいな表現や相手を侮辱する表現などが格納されている。

【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００４７
【補正方法】変更
【補正内容】
【００４７】次に、検閲者４０２はワークステーション４０５の外部記憶装置５１３にある検閲プログラム１１０１に、ステップ１３０６で改ざんされていないことを確認された通信内容を与えて、ワークステーション４０５のメモリ５０５上で実行させて、検閲後の通信内容を得る。ここで、通信内容の検閲は、検閲プログラム１１０１で行わないで、人間である検閲者が手動で行う場合も想定している（ステップ１３０７）。

【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００５１
【補正方法】変更
【補正内容】
【００５１】次に、送信者４０１はワークステーション４０４の外部記憶装置５１３にあるデジタル署名検証プログラム５０８に、ステップ１３１０で受信した２つの通信データをそれぞれ個別に与えて、ワークステーション４０４のメモリ５０５上で実行させ、通信データ内の通信内容が改ざんされていないか確認する。どちらか一方の通信内容が改ざんされていればステップ１３２１へ進む。どちらも改ざんされていなければステップ１３１２へ進む（ステップ１３１１）。

【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００５３
【補正方法】変更
【補正内容】
【００５３】次に、送信者４０１はステップ１３１０で受信した２つの通信データのコピーを外部記憶装置５１３の履歴テーブルに格納する（ステップ１３１３）。

【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００６３
【補正方法】変更
【補正内容】
【００６３】改ざんがあった場合、送信者４０１、検閲者４０２、受信者４０３、いづれの場合も通信データを全て消去する（ステップ１３２１）。

【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００８０
【補正方法】変更
【補正内容】
【００８０】ステップ１７０２で取り出したワードデータをキーに与えられた通信内容を検索する。検索がマッチすればステップ１７０４へ、通信内容を最後まで検索したらステップ１７０５へ進む（ステップ１７０３）。通信内容の検索がマッチしたワードの全文字を検閲文字に置き換える。そして、ステップ１７０３へ戻る（ステップ１７０４）。